

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2002-23999
(P2002-23999A)

(43)公開日 平成14年1月25日(2002.1.25)

(51)Int.Cl. ⁷	識別記号	F I	テマコード*(参考)
G 0 6 F 7/552		G 0 6 F 7/552	A 5 J 1 0 4
		7/72	
G 0 9 C 1/00	6 5 0	G 0 9 C 1/00	6 5 0 A

審査請求 有 請求項の数33 O L (全 22 頁)

(21)出願番号 特願2000-185582(P2000-185582)

(22)出願日 平成12年6月21日(2000.6.21)

(71)出願人 390009531

インターナショナル・ビジネス・マシー
ズ・コーポレーション

INTERNATIONAL BUSIN
ESS MACHINES CORPO
RATION

アメリカ合衆国10504、ニューヨーク州

アーモンク (番地なし)

(74)復代理人 100110607

弁理士 間山 進也 (外3名)

最終頁に続く

(54)【発明の名称】 乗算モジュール、乗法逆元演算回路、乗法逆元演算制御方式、該乗法逆元演算を用いる装置、暗号装置、誤り訂正復号器

(57)【要約】 (修正有)

【課題】 ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するための乗算モジュールを提供する。

【解決手段】 第1の入力部からの第1の m ビットデータが入力される第1および第2のべき乗演算手段 $U1$ 、 $U2$ と、第1の m ビットデータおよび第1のべき乗演算手段からの出力が入力される第1の乗算手段 $U3$ と、第2の入力部からの第2の m ビットデータおよび第2のべき乗演算手段 $U2$ からの出力が入力される第2の乗算手段 $U4$ と、第2の乗算手段の出力信号および第2の m ビットデータが入力される選択手段 $U5$ と、第1のべき乗演算手段には第1の制御信号 $S1$ が入力され、第2のべき乗演算手段には第2の制御信号 $S2$ が入力され、選択手段には該選択手段の出力を制御するための第3の制御信号 $S0$ が入力され、前記第1の乗算手段が第1の出力信号を出力し、前記選択手段が第2の出力信号を出力する。

基本演算モジュール

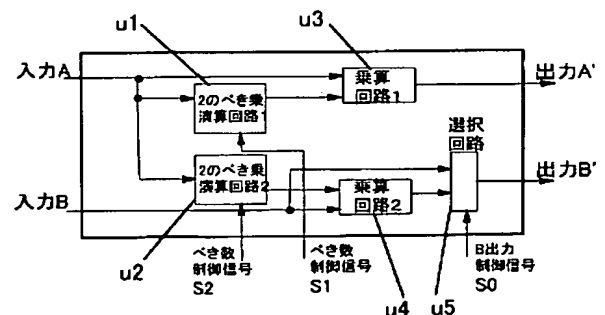


図4 回路の構成に用いる乗算デバイス

【特許請求の範囲】

【請求項 1】 ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するための第 1 の入力部と第 2 の入力部とを含む乗算モジュールであって、

前記第 1 の入力部からの第 1 の m ビットデータが入力される第 1 および第 2 のべき乗演算手段と、

前記第 1 の m ビットデータおよび前記第 1 のべき乗演算手段からの出力が入力される第 1 の乗算手段と、

前記第 2 の入力部からの第 2 の m ビットデータおよび前記第 2 のべき乗演算手段からの出力が入力される第 2 の乗算手段と、

前記第 2 の乗算手段の出力信号および前記第 2 の m ビットデータが入力される選択手段と、

前記第 1 のべき乗演算手段と、前記第 2 のべき乗演算手段と、前記選択手段とにそれぞれ制御信号を出力する制御手段とを含んで構成され、

前記第 1 のべき乗演算手段には第 1 の制御信号が入力され、前記第 2 のべき乗演算手段には第 2 の制御信号が入力され、前記選択手段には該選択手段の出力を制御するための第 3 の制御信号が入力され、前記第 1 の乗算手段が第 1 の出力信号を出力し、前記選択手段が第 2 の出力信号を出力する、乗算モジュール。

【請求項 2】 請求項 1 の乗算モジュールと、第 1 の初期値が設定でき前記乗算モジュールの第 1 の出力信号が入力される、第 1 のレジスタ手段と、第 2 の初期値が設定でき前記乗算モジュールの第 2 の出力信号が入力される、第 2 のレジスタ手段とを含み、前記第 1 のレジスタ手段の出力が前記乗算モジュールの第 1 の入力部に接続され、前記第 2 のレジスタ手段の出力が前記乗算モジュールの第 2 の入力部に接続されており、

前記第 2 のレジスタ手段が、前記第 1、第 2、第 3 の制御信号に応じて前記第 1 の初期値の乗法逆元を与える、乗法逆元演算回路。

【請求項 3】 前記第 1 の初期値と前記第 2 の初期値とをレジスタ手段へ入力し、前記制御手段は、サイクル数が所定の数 k (k は、自然数) となった場合に第 1 のべき乗演算手段に $r = 2^{k-1}$ 、 $s = 2^r$ として s 乗を計算させる第 1 の制御信号と、第 2 のべき乗演算手段に $r = \{(m-1) \bmod (2^{k-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第 2 の制御信号とを入力し、前記乗算モジュールの選択手段には、 $(m-1)$ の 2 進表現でのビット $k-1$ が 1 の場合には前記第 2 のレジスタ手段の出力に前記第 2 の乗算手段の出力を入力し、 $(m-1)$ の 2 進表現でのビット $k-1$ が 1 でない場合には前記第 2 のレジスタ手段の出力に前記第 2 のレジスタ手段の出力を与える第 3 の制御信号を入力する、請求項 2 に記載の乗法逆元演算回路。

【請求項 4】 請求項 1 の乗算モジュール 2 個と、第 1 の初期値が設定できる第 1 のレジスタ手段と、第 2 の初

期値が設定できる第 2 のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第 1 の出力を他の前記第 1 の入力部に接続し、前記乗算モジュールのそれぞれ第 2 の出力を他の前記第 2 の入力部に接続し、

前記乗算モジュール群の結合によって得られた回路に対し、前記乗算モジュールの第 1 の入力部に前記第 1 のレジスタ手段の出力が接続され、前記乗算モジュールの第 2 の入力部に前記第 2 のレジスタ手段の出力が接続され、前記乗算モジュールの第 1 の出力部に前記第 1 のレジスタ手段の入力が接続され、前記乗算モジュールの第 2 の出力部に前記第 2 のレジスタ手段の入力が接続された乗法逆元演算回路。

【請求項 5】 3 個以上の請求項 1 の乗算モジュールと、第 1 の初期値が設定できる第 1 のレジスタ手段と、第 2 の初期値が設定できる第 2 のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第 1 の出力を他の前記第 1 の入力部に接続し、前記乗算モジュールのそれぞれ第 2 の出力を他の前記第 2 の入力部に接続し、前記乗算モジュール群の結合によって得られた回路に対し、前記乗算モジュールの第 1 の入力部に前記第 1 のレジスタ手段の出力が接続され、前記乗算モジュールの第 2 の入力部に前記第 2 のレジスタ手段の出力が接続され、前記乗算モジュールの第 1 の出力部に前記第 1 のレジスタ手段の入力が接続され、前記乗算モジュールの第 2 の出力部に前記第 2 のレジスタ手段の入力が接続された乗法逆元演算回路。

【請求項 6】 前記乗算モジュールの数 n (n は、自然数) は、 $\lceil \log_2(m-1) \rceil + 1$ 以下とされる、請求項 4 または 5 に記載の乗法逆元演算回路。

【請求項 7】 制御手段により、 i 段目 ($n \geq i \geq 1$) の乗算モジュールに対して、サイクル数が所定の数 q (q は自然数) となった場合に、 $p = \{n(q-1) + i\}$ として、第 1 のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第 1 の制御信号と、第 2 のべき乗演算手段に $r = \{(m-1) \bmod (2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第 2 の制御信号とを入力し、前記 i 段目の乗算モジュールの選択手段には、 $(m-1)$ の 2 進表現でのビット $p-1$ が 1 の場合には前記 i 段目の乗算モジュールの第 2 の出力に前記第 2 の乗算手段の出力を与え、 $(m-1)$ の 2 進表現でのビット $p-1$ が 1 でない場合には前記 i 段目のモジュールの第 2 の出力に、前記 i 段目の乗算モジュールへの第 2 の入力部からの m ビットデータを与える第 3 の制御信号を入力する、請求項 4、5 または 6 に記載の乗法逆元演算回路。

【請求項 8】 $\lceil \log_2(m-1) \rceil + 1$ 個の請求項 1 の乗算モジュールと、それぞれの前記乗算モジュールを制御するための第 1 の制御信号群と、第 2 の制御信号群と、第 3 の制御信号群とを与える制御手段とを含み、

3.

前記乗算モジュールのそれぞれ第1の出力が次の前記乗算モジュールの第1の入力部に接続され、前記乗算モジュールのそれぞれ第2の出力が次の前記乗算モジュールの前記第2の入力部に接続されており、

前記制御手段は、所定段目 k (k は、自然数) の乗算モジュールに対して、 $r = 2^{k-1}$ 、 $s = 2^r$ として s 乗を計算させる第1の制御信号を第1のべき乗演算手段に与え、 $r = \{(m-1) \bmod (2^{k-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第2の制御信号を第2のべき乗演算手段に与え、 $m-1$ の2進表現におけるビット $k-1$ が1の場合に選択手段の出力として第2の乗算手段の出力を与え、 $m-1$ の2進表現におけるビット $k-1$ が1ではない場合には選択手段の出力として第2の入力部から入力される m ビットデータを与える、乗法逆元演算回路。

【請求項9】 前記乗算モジュールに接続される対となったレジスタ手段を含む、請求項8に記載の乗法逆元演算回路。

【請求項10】 ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するための第1の入力部と第2の入力部とを含む乗算モジュールの制御方式であって、第1および第2のべき乗演算手段に前記第1の入力部からの第1の m ビットデータを入力する段階と、第1の乗算手段に前記第1の m ビットデータおよび前記第1のべき乗演算手段からの出力を入力する段階と、第2の乗算手段に前記第2の入力部からの第2の m ビットデータおよび前記第2のべき乗演算手段からの出力を入力する段階と、

選択手段に前記第2の乗算手段の出力信号および前記第2の m ビットデータを入力する段階と、制御回路から前記第1の乗算手段と、前記第2の乗算手段と、前記選択手段とにそれぞれ制御信号を出力する段階とを含む、

前記第1のべき乗演算手段に第1の制御信号を入力し、前記第2のべき乗演算手段に第2の制御信号を入力し、前記選択手段に該選択手段の出力を制御するための第3の制御信号を入力し、前記第1の乗算手段に第1の出力信号を出力させ、前記選択手段に第2の出力信号を出力させる、乗算モジュールの制御方式。

【請求項11】 請求項1の乗算モジュールを与える段階と、第1の初期値が設定でき前記乗算モジュールの第1の出力信号が入力される、第1のレジスタ手段を与える段階と、第2の初期値が設定でき前記乗算モジュールの第2の出力信号が入力される、第2のレジスタ手段を与える段階とを含む、前記第1のレジスタ手段の出力が前記乗算モジュールの第1の入力部に接続され、前記第2のレジスタ手段の出力が前記乗算モジュールの第2の入力部に接続されており、

4.

さらに、前記第2のレジスタ手段が、前記第1、第2、第3の制御信号に応じて前記第1の初期値の乗法逆元を与える段階とを含む、乗法逆元演算回路の制御方式。

【請求項12】 前記第1の初期値と前記第2の初期値とを入力する段階と、サイクル数が所定の数 k (k は、自然数) となった場合に第1のべき乗演算手段に $r = 2^{k-1}$ 、 $s = 2^r$ として s 乗を計算させる第1の制御信号と、第2のべき乗演算手段に $r = \{(m-1) \bmod (2^{k-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第2の制御信号とを入力し、前記乗算モジュールの選択手段には、 $(m-1)$ の2進表現でのビット $k-1$ が1の場合には前記第2のレジスタ手段の入力に前記第2の乗算手段の出力を入力し、 $(m-1)$ の2進表現でのビット $k-1$ が1でない場合には前記第2のレジスタ手段の入力に前記第2のレジスタ手段の出力を入力するための第3の制御信号を入力する段階を含む、請求項11に記載の乗法逆元演算回路の制御方式。

【請求項13】 請求項1の乗算モジュール2個と、第1の初期値が設定できる第1のレジスタ手段と、第2の初期値が設定できる第2のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第1の出力を他の前記第1の入力部に接続し、前記乗算モジュールのそれぞれ第2の出力を他の前記第2の入力部に接続した乗法逆元演算回路の制御方式であって、前記乗算モジュールの第1の出力部に前記第1のレジスタ手段の入力が接続され、前記乗算モジュールの第2の出力部に前記第2のレジスタ手段の入力が接続され、

前記乗算モジュール群の結合によって得られた回路に対し、前記乗算モジュールの第1の入力部に前記第1のレジスタ手段の出力を接続する段階と、前記乗算モジュールの第2の入力部に前記第2のレジスタ手段の出力を接続する段階と、を含む、乗法逆元演算回路の制御方式。

【請求項14】 3個以上の請求項1の乗算モジュール2個と、第1の初期値が設定できる第1のレジスタ手段と、第2の初期値が設定できる第2のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第1の出力を他の前記第1の入力部に接続し、前記乗算モジュールのそれぞれ第2の出力を他の前記第2の入力部に接続した乗法逆元演算回路の制御方式であって、前記乗算モジュールの第1の出力部に前記第1のレジスタ手段の入力が接続され、前記乗算モジュールの第2の出力部に前記第2のレジスタ手段の入力が接続され、

前記乗算モジュール群の結合によって得られた回路に対し、前記乗算モジュールの第1の入力部に前記第1のレジスタ手段の出力を接続する段階と、前記乗算モジュールの第2の入力部に前記第2のレジスタ手段の出力を接続する段階とを含む、乗法逆元演算回路の制御方式。

【請求項15】 前記乗算モジュールの数 n (n は、自然数) は、 $\lceil \log_2(m-1) \rceil + 1$ 以下とされる、請求項13または14に記載の乗法逆元演算回路の制御方式。

【請求項 16】 i 段目 ($n \geq i \geq 1$) の乗算モジュールに対して、サイクル数が所定の数 q (q は自然数) となった場合に、 $p = \{n(q-1) + i\}$ として、第 1 のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第 1 の制御信号と、第 2 のべき乗演算手段に $r = \{(m-1) \bmod (2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第 2 の制御信号とを入力し、前記乗算モジュールの選択手段には、 $(m-1)$ の 2 進表現でのビット $p-1$ が 1 の場合には前記 i 段目の乗算モジュールの第 2 の出力に前記第 2 の乗算手段の出力を与え、 $(m-1)$ の 2 進表現でのビット $p-1$ が 1 でない場合には前記 i 段目の乗算モジュールの第 2 の出力に、前記 i 段目の乗算モジュールの第 2 の入力部からの m ビットデータを与える第 3 の制御信号を入力する、請求項 13、14 または 16 に記載の乗法逆元演算回路の制御方式。

【請求項 17】 $\lceil \log_2(m-1) \rceil + 1$ 個の請求項 1 の乗算モジュールを与える段階と、
それぞれの前記乗算モジュールを制御するための第 1 の制御信号群と、第 2 の制御信号群と、第 3 の制御信号群とを与える段階とを含み、前記乗算モジュールのそれぞれ前記第 1 の出力が次の前記第 1 の入力部に接続され、前記乗算モジュールのそれぞれ前記第 2 の出力が次の前記第 2 の入力部に接続されており、
所定段目 k (k は、自然数) の乗算モジュールに対して、 $r = 2^{k-1}$ 、 $s = 2^r$ として s 乗を計算させる第 1 の制御信号を第 1 のべき乗演算手段に与え、 $r = \{(m-1) \bmod (2^{k-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第 2 の制御信号を第 2 のべき乗演算手段に与え、 $m-1$ の 2 進表現におけるビット $k-1$ が 1 の場合には選択手段の出力として第 2 の乗算手段の出力を与え、 $m-1$ の 2 進表現におけるビット $k-1$ が 1 でない場合には選択手段の出力として第 2 の入力部から入力される m ビットデータを与える段階を含む、乗法逆元演算回路の制御方式。

【請求項 18】 前記乗算モジュールからの出力を対となったレジスタ手段に入力する段階を含む、請求項 12、13、または 14 に記載の乗法逆元演算回路。

【請求項 19】 ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するための第 1 の入力部と第 2 の入力部とを含む乗算モジュールを用いる装置であって、該乗算モジュールは、
前記第 1 の入力部からの第 1 の m ビットデータが入力される第 1 および第 2 のべき乗演算手段と、
前記第 1 の m ビットデータおよび前記第 1 のべき乗演算手段からの出力が入力される第 1 の乗算手段と、
前記第 2 の入力部からの第 2 の m ビットデータおよび前記第 2 のべき乗演算手段からの出力が入力される第 2 の乗算手段と、
前記第 2 の乗算手段の出力信号および前記第 2 の m ビッ

トデータが入力される選択手段と、

前記第 1 のべき乗演算手段と、前記第 2 のべき乗演算手段と、前記選択手段とにそれぞれ制御信号を出力する制御回路とを含んで構成され、

前記第 1 のべき乗演算手段には第 1 の制御信号が入力され、前記第 2 のべき乗演算手段には第 2 の制御信号が入力され、前記選択手段には該選択手段の出力を制御するための第 3 の制御信号が入力され、前記第 1 の乗算手段が第 1 の出力信号を出力し、前記選択手段が第 2 の出力信号を出力する装置。

【請求項 20】 請求項 1 の乗算モジュールと、
第 1 の初期値が設定でき前記乗算モジュールの第 1 の出力信号が入力される、第 1 のレジスタ手段と、
第 2 の初期値が設定でき前記乗算モジュールの第 2 の出力信号が入力される、第 2 のレジスタ手段とを含み、
前記第 1 のレジスタ手段の出力が前記乗算モジュールの第 1 の入力部に接続され、前記第 2 のレジスタ手段の出力が前記乗算モジュールの第 2 の入力部に接続されており、

前記第 2 のレジスタ手段が、前記第 1、第 2、第 3 の制御信号に応じて前記第 1 の初期値の乗法逆元を与える、乗法逆元演算回路を含む装置。

【請求項 21】 前記第 1 の初期値と前記第 2 の初期値とを入力し、サイクル数が所定の数 k (k は、自然数) となった場合に第 1 のべき乗演算手段に $r = 2^{k-1}$ 、 $s = 2^r$ として s 乗を計算させる第 1 の制御信号と、第 2 のべき乗演算手段に $r = \{(m-1) \bmod (2^{k-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第 2 の制御信号とを入力し、前記乗算モジュールの選択手段には、 $(m-1)$ の 2 進表現でのビット $k-1$ が 1 の場合には前記第 2 のレジスタ手段の入力に前記第 2 の乗算手段の出力を入力し、 $(m-1)$ の 2 進表現でのビット $k-1$ が 1 でない場合には前記第 2 のレジスタ手段の入力に前記第 2 のレジスタ手段の出力を入力するための第 3 の制御信号を入力する、乗法逆元演算回路を含む請求項 20 に記載の装置。

【請求項 22】 請求項 1 の乗算モジュール 2 個と、第 1 の初期値が設定できる第 1 のレジスタ手段と、第 2 の初期値が設定できる第 2 のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第 1 の出力を他の前記第 1 の入力部に接続し、前記乗算モジュールのそれぞれ第 2 の出力を他の前記第 2 の入力部に接続し、
前記乗算モジュール群の結合によって得られた回路に対し、その第 1 の入力部に前記第 1 のレジスタ手段の出力が接続され、前記乗算モジュールの第 2 の入力部に前記第 2 のレジスタ手段の出力が接続され、前記乗算モジュールの第 1 の出力部に前記第 1 のレジスタ手段の入力が接続され、前記乗算モジュールの第 2 の出力部に前記第 2 のレジスタ手段の入力が接続された乗法逆元演算回路を含む、装置。

【請求項 2 3】 3 個以上の請求項 1 の乗算モジュールと、第 1 の初期値が設定できる第 1 のレジスタ手段と、第 2 の初期値が設定できる第 2 のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第 1 の出力を他の前記第 1 の入力部に接続し、前記乗算モジュールのそれぞれ第 2 の出力を他の前記第 2 の入力部に接続し、前記乗算モジュール群の結合によって得られた回路に対し、その第 1 の入力部に前記第 1 のレジスタ手段の出力が接続され、前記乗算モジュールの第 2 の入力部に前記第 2 のレジスタ手段の出力が接続され、前記乗算モジュールの第 1 の出力部に前記第 1 のレジスタ手段の入力が接続され、前記乗算モジュールの第 2 の出力部に前記第 2 のレジスタ手段の入力が接続された乗法逆元演算回路を含む、装置。

【請求項 2 4】 前記乗算モジュールの数 n (n は、自然数) は、 $\lceil \log_2(m-1)+1 \rceil$ 以下とされる乗法逆元演算回路を含む請求項 2 2 または 2 3 に記載の装置。

【請求項 2 5】 前記制御手段により、 i 段目 ($n \geq i \geq 1$) の乗算モジュールに対して、サイクル数が所定の数 q (q は自然数) となった場合に、 $p = \{n(q-1) + i\}$ として、第 1 のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第 1 の制御信号と、第 2 のべき乗演算手段に $r = \{(m-1) \bmod (2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算する第 2 の制御信号とを入力し、前記 i 番目の乗算モジュールの選択手段には、 $(m-1)$ の 2 進表現でのビット $p-1$ が 1 の場合には前記 i 番目の乗算モジュールの第 2 の出力に前記第 2 の乗算手段の出力を与え、 $(m-1)$ の 2 進表現でのビット $p-1$ が 1 でない場合には前記 i 番目の乗算モジュールの第 2 の出力を、前記 i 段目の乗算モジュールの第 2 の入力部からの m ビットデータとする第 3 の制御信号を入力する乗法逆元演算回路を含む、請求項 2 2、2 3 または 2 4 に記載の装置。

【請求項 2 6】 $\lceil \log_2(m-1)+1 \rceil$ 個の請求項 1 の乗算モジュールと、それぞれの前記乗算モジュールを制御するための第 1 の制御信号群と、第 2 の制御信号群と、第 3 の制御信号群とを与える制御手段とを含み、前記乗算モジュールのそれぞれ第 1 の出力が他の前記乗算モジュールの第 1 の入力部に接続され、前記乗算モジュールのそれぞれ第 2 の出力が他の前記乗算モジュールの第 2 の入力部に接続されており、前記制御手段は、所定段目 k (k は、自然数) の乗算モジュールに対して、 $r = 2^{k-1}$ 、 $s = 2^r$ として s 乗を計算させる第 1 の制御信号を第 1 のべき乗演算手段に与え、 $r = \{(m-1) \bmod (2^{k-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第 2 の制御信号を第 2 のべき乗演算手段に与え、 $m-1$ の 2 進表現におけるビット $k-1$ が 1 の場合に選択手段の出力として第 2 の乗算手段の出力を与え、 $m-1$ の 2 進表現におけるビット $k-1$

が 1 ではない場合には選択手段の出力として前記第 2 の入力部から入力される m ビットデータを与える乗法逆元演算回路を含む装置。

【請求項 2 7】 前記乗算モジュールに接続される対となったレジスタ手段を含む、請求項 2 2、2 3 または 2 4 に記載の乗法逆元演算回路を含む装置。

【請求項 2 8】 ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するため、第 1 の入力部から m ビットデータおよびべき乗演算手段からの出力を乗算手段に入力する段階と、第 2 の入力部からの m ビットデータおよび前記べき乗演算手段からの出力を乗算手段に入力する段階とを含む乗法逆元演算回路の制御方式であって、 $p = \{n(q-1) + i\}$ として、第 1 のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第 1 の制御信号と、第 2 のべき乗演算手段に $r = \{(m-1) \bmod (2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算する第 2 の制御信号とを入力する段階と、 $m-1$ の 2 進表現におけるビット $k-1$ (k は、自然数) が 1 の場合に選択手段の出力として第 2 の乗算手段の出力を与え、 $m-1$ の 2 進表現におけるビット $k-1$ が 1 ではない場合には選択手段の出力として前記第 2 の入力部から入力される m ビットデータを与える段階とを含む、乗法逆元演算回路の制御方式。

【請求項 2 9】 ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するため、第 1 の入力部から m ビットデータおよびべき乗演算手段からの出力を乗算手段に入力する段階と、第 2 の入力部からの m ビットデータおよび前記べき乗演算手段からの出力を乗算手段に入力する段階とを含む乗算方法を実行させるためのソースコードが記録されたコンピュータ可読な記録媒体であって、該記録媒体は、 $p = \{n(q-1) + i\}$ として、第 1 のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第 1 の制御信号と、第 2 のべき乗演算手段に $r = \{(m-1) \bmod (2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算する第 2 の制御信号とを入力し、 $m-1$ の 2 進表現におけるビット $k-1$ (k は、自然数) が 1 の場合に選択手段の出力として第 2 の乗算手段の出力を与え、 $m-1$ の 2 進表現におけるビット $k-1$ が 1 ではない場合には選択手段の出力として前記第 2 の入力部から入力される m ビットデータを与える、記録媒体。

【請求項 3 0】 ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するため、第 1 の入力部から m ビットデータおよびべき乗演算手段からの出力を乗算手段に入力する段階と、第 2 の入力部からの m ビットデータおよび前記べき乗演算手段からの出力を乗算手段に入力する段階とを含む乗算方法を実行させるためのソースコードが記録されたコンピュータ可読な伝送媒体であって、該伝送媒体は、

$p = \{n(q-1) + i\}$ として、第 1 のべき乗演算手

段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第 1 の制御信号と、第 2 のべき乗演算手段に $r = \{(m-1) \bmod (2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算する第 2 の制御信号とを入力し、
 $m-1$ の 2 進表現におけるビット $k-1$ (k は、自然数) が 1 の場合に選択手段の出力として第 2 の乗算手段の出力を与え、 $m-1$ の 2 進表現におけるビット $k-1$ が 1 ではない場合には選択手段の出力として前記第 2 の入力部から入力される m ビットデータを与える、伝送媒体。

【請求項 3 1】 ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するため、第 1 の入力部からの m ビットデータおよびべき乗演算手段からの出力が入力される乗算手段と、第 2 の入力部からの m ビットデータおよび前記べき乗演算手段からの出力が入力される乗算手段とを含む暗号装置であって、

$p = \{n(q-1) + i\}$ として、第 1 のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第 1 の制御信号と、第 2 のべき乗演算手段に $r = \{(m-1) \bmod (2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第 2 の制御信号とを入力するための手段と、
 $m-1$ の 2 進表現におけるビット $k-1$ (k は、自然数) が 1 の場合に選択手段の出力として第 2 の乗算手段の出力を与え、 $m-1$ の 2 進表現におけるビット $k-1$ が 1 ではない場合には選択手段の出力として前記第 2 の入力部から入力される m ビットデータを与えるための手段と、を含む暗号装置。

【請求項 3 2】 ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するため、第 1 の入力部からの m ビットデータおよびべき乗演算手段からの出力が入力される乗算手段と、第 2 の入力部からの m ビットデータおよび前記べき乗演算手段からの出力が入力される乗算手段とを含む誤り訂正復号器であって、

$p = \{n(q-1) + i\}$ として、第 1 のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第 1 の制御信号と、第 2 のべき乗演算手段に $r = \{(m-1) \bmod (2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算する第 2 の制御信号とを入力するための手段と、
 $m-1$ の 2 進表現におけるビット $k-1$ (k は、自然数) が 1 の場合に選択手段の出力として第 2 の乗算手段の出力を与え、 $m-1$ の 2 進表現におけるビット $k-1$ が 1 ではない場合には選択手段の出力として前記第 2 の入力部から入力される m ビットデータを与えるための手段と、を含む誤り訂正復号器。

【請求項 3 3】 ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するため、第 1 の入力部からの m ビットデータおよびべき乗演算手段からの出力が入力される乗算手段と、第 2 の入力部からの m ビットデータおよび前記べき乗演算手段からの出力が入力される乗算手段とを含む装置であって、

$p = \{n(q-1) + i\}$ として、第 1 のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第 1 の制御信号と、第 2 のべき乗演算手段に $r = \{(m-1) \bmod (2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算する第 2 の制御信号とを入力するための手段と、
 $m-1$ の 2 進表現におけるビット $k-1$ (k は、自然数) が 1 の場合に選択手段の出力として第 2 の乗算手段の出力を与え、 $m-1$ の 2 進表現におけるビット $k-1$ が 1 ではない場合には選択手段の出力として前記第 2 の入力部から入力される m ビットデータを与えるための手段と、を含む装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、乗算モジュール、乗法逆元演算回路、乗法逆元演算回路の制御方式、および装置に関し、より詳細には、ガロア拡大体 $GF(2^m)$ (m は任意の自然数) の乗法逆元演算を、低レイテンシかつ小規模な回路によって実現することを可能とする乗算モジュール、乗法逆元演算回路、乗法逆元演算回路の制御方式、装置、暗号装置および誤り訂正復号器に関する。

【0002】

【従来の技術】まず、本発明も含めて、ハードウェア向けの逆数演算アルゴリズムの評価ポイントは次のとおり：

(1) 乗算器の個数

(2) レジスタの個数

(3) レイテンシ (順序回路の場合はクロック数 * クロック周波数)。これは行う乗算の回数に強く依存する。

(4) 順序回路の場合、最大動作周波数。当然ながら、同じクロック数で計算ができるなら、最大動作周波数が高い回路がよい。同じ最大動作周波数なら、少ないクロック数で計算ができる回路がよい。

上記の各ポイントについて従来手法や本発明がどうかは、後に比較として述べるので、以下では従来手法の概要についてまずまとめる。

【0003】方法 1: Fermat's little theorem

文献[1]や[4]などに示されているとおり、

【0004】

【数 1】

$$x^{-1} = x^{2^m-2} = x^{2^1} x^{2^2} \cdots x^{2^{m-1}}$$

の公式 (Fermat の小定理) を用いて乗法逆元を計算できる。この式のとおりに計算を進めると、 $m-2$ 回の乗算が必要である。

【0005】この公式の計算を順序回路として作る場合には、図 1 に示した計算過程に基づいて、1 個の乗算回路と 1 個の 2 乗回路を持ち、 (x^2) の i 乗を求めながら $(m-2)$ 回のループで計算するアルゴリズムがよく使われている。レイテンシ (サイクル数) は $(m-2)$

となる。

【0006】組み合わせ回路で実現する場合は、図2のように木構造を作れば、Mを乗算回路のレイテンシとして

【0007】

【数2】

$$M \{ \lceil \log_2 (m-2) + 1 \rceil \}$$

のレイテンシとなる（一般に、べき乗演算のレイテンシはごく小さいので無視する）。

【0008】方法2：伊東・辻井のアルゴリズムと、その類似手法

文献[2]に、これまで知られている限りもっとも乗算回数が少なく済むアルゴリズム（伊東・辻井のアルゴリズム）が示されている。図3に $m=16$ における計算過程の例を示す。また、このアルゴリズムより以前に伊東らが文献[3]で提案した別アルゴリズムに、

【0009】

【数3】

$$2^k - 1 = 2 \left(2^{k/2} - 1 \right) \left(2^{k/2} + 1 \right)$$

等の関係を用いてべき数 $2^m - 2$ を再帰的に2分解し、実計算はその逆の手順でボトムアップに乗算およびべき乗演算を進める、という方法もある。いずれのアルゴリズムでも、順序回路にしたときサイクル数は、

【0010】

【数4】

$$\lceil \log_2 (m-1) \rceil + Hw(m-1) - 1$$

であり、組み合わせ回路にしたときレイテンシは、Mを乗算回路のレイテンシとして

【0011】

【数5】

$$M \{ \lceil \log_2 (m-1) \rceil + Hw(m-1) - 1 \}$$

となる（べき乗演算のレイテンシは、ごく小さいので無視した）。

【0012】いずれのアルゴリズムでも、方法1と異なり、各乗算を逐次的に進めないと正しい計算結果が得られないという問題点がある。

【0013】方法3：乗算と部分体上での乗法逆元演算の組み合わせによる方法

文献[4]、[2]などに、 $GF(2^m)$ において $m=kq$ （ m が合成数）であるとき、 $GF(2^m)$ の乗法逆元演算を $GF(2^m)$ の乗算と $GF(2^k)$ （ないし $GF(2^q)$ ）の乗法逆元演算に帰着する方法が示されている。これにより、うまく原始多項式や表現基底を選定すれば、かなり回路規模が縮小され、回路速度も速くなる場合が存在する。

【0014】しかし、この方法は限られた特定の場合にしか使えないという問題がある。たとえば m が素数であればまったく使えないし、ターゲットの体 $GF(2^m)$

の原始多項式によっては、回路規模や速度の向上が得られないこともある。

【0015】方法4：ユークリッド互除法

文献[5]等では、多項式上でユークリッド互除法を用いて乗法逆元を計算する方法が示されている。これは、入力多項式（乗法逆元を求めたい多項式）をA、原始多項式をFとしたとき、ユークリッド互除法で $BA + FM = 1$ を満たすB、Mを求めると、ガロア体上ではBがAの乗法逆元となるという性質を利用したものである。この方法は、一般にレイテンシが $O(m)$ となるという問題点がある。

【0016】代表的な文献：

[1] S.B.Wicker and V.K.Bhargava (eds.), Reed-Solomon Codes and Their Applications, IEEE Press, 1994.

[2] T.Itoh and S.Tsujii, "A Fast Algorithm for Computing Multiplicative Inverses in $GF(2^m)$ Using Normal Bases," Information and Computation, vol.78, no.3, pp.171-177, 1988.

[3] T.Itoh, O.Teechai and S.Tsujii, "A fast algorithm for computing multiplicative inverses in $GF(2^m)$ using normal bases, J. Society for Electronic Communications (Japan), 44, 31-36, 1986.

[4] J.Guajardo and C.Paar, "Efficient Algorithms for Elliptic Curve Cryptosystems," proc. of 17th Annual Intl. Cryptology Conf. (CRYPTO'97), LNCS1294, pp.342-356, 1997.

[5] H.Brunner, A.Curiger and M.Hofstetter, "On computing multiplicative inverses in $GF(2^m)$," IEEE Trans. Computers, vol.42, pp.1010-1015, 1993.

30 【0017】

【発明が解決しようとする課題】伊東のアルゴリズムでは、乗算回数は少ないが、回路のレイテンシが大きくなるという問題がある。逆にFermatでは、組み合わせ回路にしたとき、レイテンシは小さいが回路規模が大きくなり、順序回路にしたとき、レイテンシが大きくなる、という問題がある。

【0018】本発明では両方の手法の良い部分を取り、順序回路、組み合わせ回路のいずれの場合についても、小規模、低レイテンシを、一度に達成する。本発明は、通常回路設計で良くあるようなスピードとエリアのトレードオフを図る話ではなく、それらを両方改善するのである。

【0019】本発明は、任意の m を対象として、基本モジュールを組み合わせた形で、低いレイテンシ（順序回路の場合は少ない処理クロック数、組み合わせ回路の場合は少ディレイ）を乗算回数を増やすことなく達成するものである。既存の方法では、いずれもレイテンシを減らすこと自体が困難か、レイテンシを減らそうとすると回路規模がたいへん大きくなるという問題があった。具体的には、以下の通りである。

13.

【0020】(1) Fermatの定理をそのまま計算する方法では、組み合わせ回路にすればレイテンシは、

【0021】

【数6】

$$M\{\lceil \log_2(m-2) \rceil + 1\}$$

にまで改善できるが、乗算回路が $m-2$ 個必要となる。

【0022】(2) 伊東・辻井の方法、およびその類似手法では、全体として行われる乗算の回数は、

【0023】

【数7】

$$M(\lceil \log_2(m-1) \rceil + Hw(m-1) - 1)$$

となり、Fermatよりも悪い。

【0026】(4) 部分体上の除算へ帰着する方法は、限られた m や原始多項式でしか使えない。なお、この方法は本発明と対立する手法ではなく、本手法と組み合わせ併用すれば、さらに回路性能を改善できる。

【0027】(5) ユークリッド互除法による方法は、 $O(m)$ のレイテンシがかかり、その改善は簡単でないという問題点がある。

【0028】本手法は、乗算の全回数が伊東・辻井とまったく同じ (Fermatより少ない) にも関わらず、レイテンシが最高で伊東・辻井の約半分 (Fermatと同じ) に改善できる。

【0029】

【課題を解決するための手段】乗法逆元計算は乗算やべき乗演算を利用して行うが、計算の進め方によって得られる回路の性能が変わる。本発明は、基本モジュールを組み合わせた形で、低いレイテンシ (順序回路の場合は少ない処理クロック数、組み合わせ回路の場合は少ディレイ) を乗算回数を増やすことなく達成するものである。

【0030】すなわち、本発明の上記課題は、本発明の乗算モジュール、乗法逆元演算回路、該乗法逆元演算回路の制御方式、装置、暗号装置および誤り訂正復号器を提供することにより解決される。

【0031】すなわち、本発明の請求項1の発明によれば、ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するための第1の入力部と第2の入力部とを含む乗算モジュールであって、前記第1の入力部からの第1の m ビットデータが入力される第1および第2のべき乗演算手段と、前記第1の m ビットデータおよび前記第1のべき乗演算手段からの出力が入力される第1の乗算手段と、前記第2の入力部からの第2の m ビットデータおよび前記第2のべき乗演算手段からの出力が入力される第2の乗算手段と、前記第2の乗算手段の出力信号および前記第2の m ビットデータが入力される選択手段と、前記第1のべき乗演算手段と、前記第2のべき乗演算手段と、前記選択手段とにそれぞれ制御信号を出力する制御手段

14

$$\lceil \log_2(m-1) \rceil + Hw(m-1) - 1$$

個で済むが、レイテンシを改善することが困難である。レイテンシは、順序回路で、

【0024】

【数8】

$$\lceil \log_2(m-1) \rceil + Hw(m-1) - 1$$

サイクル、組み合わせ回路では、

10 【0025】

【数9】

とを含んで構成され、前記第1のべき乗演算手段には第1の制御信号が入力され、前記第2のべき乗演算手段には第2の制御信号が入力され、前記選択手段には該選択手段の出力を制御するための第3の制御信号が入力され、前記第1の乗算手段が第1の出力信号を出力し、前記選択手段が第2の出力信号を出力する、乗算モジュールが提供される。

20

【0032】本発明の請求項2の発明によれば、請求項1の乗算モジュールと、第1の初期値が設定でき前記乗算モジュールの第1の出力信号が入力される、第1のレジスタ手段と、第2の初期値が設定でき前記乗算モジュールの第2の出力信号が入力される、第2のレジスタ手段とを含み、前記第1のレジスタ手段の出力が前記乗算モジュールの第1の入力部に接続され、前記第2のレジスタ手段の出力が前記乗算モジュールの第2の入力部に接続されており、前記第2のレジスタ手段が、前記第1、第2、第3の制御信号に応じて前記第1の初期値の乗法逆元を与える、乗法逆元演算回路が提供される。

30

【0033】本発明の請求項3の発明によれば、前記第1の初期値と前記第2の初期値とをレジスタ手段へ入力し、前記制御手段は、サイクル数が所定の数 k (k は、自然数) となった場合に第1のべき乗演算手段に $r = 2^{k-1}$ 、 $s = 2^r$ として s 乗を計算させる第1の制御信号と、第2のべき乗演算手段に $r = \{(m-1) \bmod (2^{k-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第2の制御信号とを入力し、前記乗算モジュールの選択手段には、 $(m-1)$ の2進表現でのビット $k-1$ が1の場合には前記第2のレジスタ手段の入力に前記第2の乗算手段の出力を入力し、 $(m-1)$ の2進表現でのビット $k-1$ が1でない場合には前記第2のレジスタ手段の入力に前記第2のレジスタ手段の出力を与える第3の制御信号を入力する、乗法逆元演算回路が提供される。

40

【0034】本発明の請求項4の発明によれば、請求項1の乗算モジュール2個と、第1の初期値が設定できる第1のレジスタ手段と、第2の初期値が設定できる第2のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第1の出力を他の前記第1の入力部に接続し、前記乗

50

15、

算モジュールのそれぞれ第2の出力を他の前記第2の入力部に接続し、前記乗算モジュール群の結合によって得られた回路に対し、前記乗算モジュールの第1の入力部に前記第1のレジスタ手段の出力が接続され、前記乗算モジュールの第2の入力部に前記第2のレジスタ手段の出力が接続され、前記乗算モジュールの第1の出力部に前記第1のレジスタ手段の入力が接続され、前記乗算モジュールの第2の出力部に前記第2のレジスタ手段の入力が接続された乗法逆元演算回路。

【0035】本発明の請求項5の発明によれば、3個以上の請求項1の乗算モジュールと、第1の初期値が設定できる第1のレジスタ手段と、第2の初期値が設定できる第2のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第1の出力を他の前記第1の入力部に接続し、前記乗算モジュールのそれぞれ第2の出力を他の前記第2の入力部に接続し、前記乗算モジュール群の結合によって得られた回路に対し、前記乗算モジュールの第1の入力部に前記第1のレジスタ手段の出力が接続され、前記乗算モジュールの第2の入力部に前記第2のレジスタ手段の出力が接続され、前記乗算モジュールの第1の出力部に前記第1のレジスタ手段の入力が接続され、前記乗算モジュールの第2の出力部に前記第2のレジスタ手段の入力が接続された乗法逆元演算回路が提供される。

【0036】本発明の請求項6の発明によれば、前記乗算モジュールの数 n (n は、自然数) は、 $\lceil \log_2(m-1) + 1 \rceil$ 以下とされる、乗法逆元演算回路が提供される。

【0037】本発明の請求項7の発明によれば、制御手段により、 i 段目 ($n \geq i \geq 1$) の乗算モジュールに対して、サイクル数が所定の数 q (q は自然数) となった場合に、 $p = \{n(q-1) + i\}$ として、第1のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第1の制御信号と、第2のべき乗演算手段に $r = \{(m-1) \bmod (2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第2の制御信号とを入力し、前記 i 段目の乗算モジュールの選択手段には、 $(m-1)$ の2進表現でのビット $p-1$ が1の場合には前記 i 段目の乗算モジュールの第2の出力に前記第2の乗算手段の出力を与え、 $(m-1)$ の2進表現でのビット $p-1$ が1でない場合には前記 i 段目のモジュールの第2の出力に、前記 i 段目の乗算モジュールへの第2の入力部からの m ビットデータを与える第3の制御信号を入力する、乗法逆元演算回路が提供される。

【0038】本発明の請求項8の発明によれば、 $\lceil \log_2(m-1) + 1 \rceil$ 個の請求項1の乗算モジュールと、それぞれの前記乗算モジュールを制御するための第1の制御信号群と、第2の制御信号群と、第3の制御信号群とを与える制御手段とを含み、前記乗算モジュールのそれぞれ第1の出力が次の前記乗算モジュールの第1の入力部に接続され、前記乗算モジュールのそれぞれ第2の出力が次の前記乗算モジュールの前記第2の入力部に接続されて

16

おり、前記制御手段は、所定段目 k (k は、自然数) の乗算モジュールに対して、 $r = 2^{k-1}$ 、 $s = 2^r$ として s 乗を計算させる第1の制御信号を第1のべき乗演算手段に与え、 $r = \{(m-1) \bmod (2^{k-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第2の制御信号を第2のべき乗演算手段に与え、 $m-1$ の2進表現におけるビット $k-1$ が1の場合には選択手段の出力として第2の乗算手段の出力を与え、 $m-1$ の2進表現におけるビット $k-1$ が1ではない場合には選択手段の出力として第2の入力部から入力される m ビットデータを与える、乗法逆元演算回路が提供される。

【0039】本発明の請求項9の発明によれば、前記乗算モジュールに接続される対となったレジスタ手段を含む、乗法逆元演算回路が提供される。

【0040】本発明の請求項10の発明によれば、ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するための第1の入力部と第2の入力部とを含む乗算モジュールの制御方式であって、第1および第2のべき乗演算手段に前記第1の入力部からの第1の m ビットデータを入力する段階と、第1の乗算手段に前記第1の m ビットデータおよび前記第1のべき乗演算手段からの出力を入力する段階と、第2の乗算手段に前記第2の入力部からの第2の m ビットデータおよび前記第2のべき乗演算手段からの出力を入力する段階と、選択手段に前記第2の乗算手段の出力信号および前記第2の m ビットデータを入力する段階と、制御回路から前記第1の乗算手段と、前記第2の乗算手段と、前記選択手段とにそれぞれ制御信号を出力する段階とを含み、前記第1のべき乗演算手段に第1の制御信号を入力し、前記第2のべき乗演算手段に第2の制御信号を入力し、前記選択手段に該選択手段の出力を制御するための第3の制御信号を入力し、前記第1の乗算手段に第1の出力信号を出力させ、前記選択手段に第2の出力信号を出力させる、乗算モジュールの制御方式が提供される。

【0041】本発明の請求項11の発明によれば、請求項1の乗算モジュールを与える段階と、第1の初期値が設定でき前記乗算モジュールの第1の出力信号が入力される、第1のレジスタ手段を与える段階と、第2の初期値が設定でき前記乗算モジュールの第2の出力信号が入力される、第2のレジスタ手段を与える段階とを含み、前記第1のレジスタ手段の出力が前記乗算モジュールの第1の入力部に接続され、前記第2のレジスタ手段の出力が前記乗算モジュールの第2の入力部に接続されており、さらに、前記第2のレジスタ手段が、前記第1、第2、第3の制御信号に応じて前記第1の初期値の乗法逆元を与える段階とを含む、乗法逆元演算回路の制御方式が提供される。

【0042】本発明の請求項12の発明によれば、前記第1の初期値と前記第2の初期値とを入力する段階と、サイクル数が所定の数 k (k は、自然数) となった場合

17、

に第1のべき乗演算手段に $r = 2^{k-1}$ 、 $s = 2^r$ として s 乗を計算させる第1の制御信号と、第2のべき乗演算手段に $r = \{(m-1) \bmod (2^{k-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第2の制御信号とを入力し、前記乗算モジュールの選択手段には、 $(m-1)$ の2進表現でのビット $k-1$ が1の場合には前記第2のレジスタ手段の入力に前記第2の乗算手段の出力を入力し、 $(m-1)$ の2進表現でのビット $k-1$ が1でない場合には前記第2のレジスタ手段の入力に前記第2のレジスタ手段の出力を入力するための第3の制御信号を入力する段階を含む、乗法逆元演算回路の制御方式が提供される。

【0043】本発明の請求項13の発明によれば、請求項1の乗算モジュール2個と、第1の初期値が設定できる第1のレジスタ手段と、第2の初期値が設定できる第2のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第1の出力を他の前記第1の入力部に接続し、前記乗算モジュールのそれぞれ第2の出力を他の前記第2の入力部に接続した乗法逆元演算回路の制御方式であって、前記乗算モジュールの第1の出力部に前記第1のレジスタ手段の入力が接続され、前記乗算モジュールの第2の出力部に前記第2のレジスタ手段の入力が接続され、前記乗算モジュール群の結合によって得られた回路に対し、前記乗算モジュールの第1の入力部に前記第1のレジスタ手段の出力を接続する段階と、前記乗算モジュールの第2の入力部に前記第2のレジスタ手段の出力を接続する段階と、を含む、乗法逆元演算回路の制御方式が提供される。

【0044】本発明の請求項14の発明によれば、3個以上の請求項1の乗算モジュール2個と、第1の初期値が設定できる第1のレジスタ手段と、第2の初期値が設定できる第2のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第1の出力を他の前記第1の入力部に接続し、前記乗算モジュールのそれぞれ第2の出力を他の前記第2の入力部に接続した乗法逆元演算回路の制御方式であって、前記乗算モジュールの第1の出力部に前記第1のレジスタ手段の入力が接続され、前記乗算モジュールの第2の出力部に前記第2のレジスタ手段の入力が接続され、前記乗算モジュール群の結合によって得られた回路に対し、前記乗算モジュールの第1の入力部に前記第1のレジスタ手段の出力を接続する段階と、前記乗算モジュールの第2の入力部に前記第2のレジスタ手段の出力を接続する段階とを含む、乗法逆元演算回路の制御方式が提供される。

【0045】本発明の請求項15の発明によれば、前記乗算モジュールの数 n (n は、自然数) は、 $[\log_2(m-1)+1]$ 以下とされる、乗法逆元演算回路の制御方式が提供される。

【0046】本発明の請求項16の発明によれば、 i 段目 ($n \geq i \geq 1$) の乗算モジュールに対して、サイクル

18

数が所定の数 q (q は自然数) となった場合に、 $p = \{n(q-1) + i\}$ として、第1のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第1の制御信号と、第2のべき乗演算手段に $r = \{(m-1) \bmod (2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第2の制御信号とを入力し、前記乗算モジュールの選択手段には、 $(m-1)$ の2進表現でのビット $p-1$ が1の場合には前記 i 段目の乗算モジュールの第2の出力に前記第2の乗算手段の出力を与え、 $(m-1)$ の2進表現でのビット $p-1$ が1でない場合には前記 i 段目の乗算モジュールの第2の出力に、前記 i 段目の乗算モジュールの第2の入力部からの m ビットデータを与える第3の制御信号を入力する、乗法逆元演算回路の制御方式が提供される。

【0047】本発明の請求項17の発明によれば、 $[\log_2(m-1)+1]$ 個の請求項1の乗算モジュールを与える段階と、それぞれの前記乗算モジュールを制御するための第1の制御信号群と、第2の制御信号群と、第3の制御信号群とを与える段階とを含み、前記乗算モジュールのそれぞれ前記第1の出力が次の前記第1の入力部に接続され、前記乗算モジュールのそれぞれ前記第2の出力が次の前記第2の入力部に接続されており、所定段目 k (k は、自然数) の乗算モジュールに対して、 $r = 2^{k-1}$ 、 $s = 2^r$ として s 乗を計算させる第1の制御信号を第1のべき乗演算手段に与え、 $r = \{(m-1) \bmod (2^{k-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第2の制御信号を第2のべき乗演算手段に与え、 $m-1$ の2進表現におけるビット $k-1$ が1の場合には選択手段の出力として第2の乗算手段の出力を与え、 $m-1$ の2進表現におけるビット $k-1$ が1ではない場合には選択手段の出力として第2の入力部から入力される m ビットデータを与える段階を含む、乗法逆元演算回路の制御方式が提供される。

【0048】本発明の請求項18の発明によれば、前記乗算モジュールからの出力を対となったレジスタ手段に入力する段階を含む、乗法逆元演算回路の制御方式が提供される。

【0049】本発明の請求項19の発明によれば、ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するための第1の入力部と第2の入力部とを含む乗算モジュールを用いる装置であって、該乗算モジュールは、前記第1の入力部からの第1の m ビットデータが入力される第1および第2のべき乗演算手段と、前記第1の m ビットデータおよび前記第1のべき乗演算手段からの出力が入力される第1の乗算手段と、前記第2の入力部からの第2の m ビットデータおよび前記第2のべき乗演算手段からの出力が入力される第2の乗算手段と、前記第2の乗算手段の出力信号および前記第2の m ビットデータが入力される選択手段と、前記第1のべき乗演算手段と、前記第2のべき乗演算手段と、前記選択手段とにそれぞれ制

19、

御信号を出力する制御回路とを含んで構成され、前記第 1 のべき乗演算手段には第 1 の制御信号が入力され、前記第 2 のべき乗演算手段には第 2 の制御信号が入力され、前記選択手段には該選択手段の出力を制御するための第 3 の制御信号が入力され、前記第 1 の乗算手段が第 1 の出力信号を出力し、前記選択手段が第 2 の出力信号を出力する装置が提供される。

【0050】本発明の請求項 20 の発明によれば、請求項 1 の乗算モジュールと、第 1 の初期値が設定でき前記乗算モジュールの第 1 の出力信号が入力される、第 1 のレジスタ手段と、第 2 の初期値が設定でき前記乗算モジュールの第 2 の出力信号が入力される、第 2 のレジスタ手段とを含み、前記第 1 のレジスタ手段の出力が前記乗算モジュールの第 1 の入力部に接続され、前記第 2 のレジスタ手段の出力が前記乗算モジュールの第 2 の入力部に接続されており、前記第 2 のレジスタ手段が、前記第 1、第 2、第 3 の制御信号に応じて前記第 1 の初期値の乗法逆元を与える、乗法逆元演算回路を含む装置が提供される。

【0051】本発明の請求項 21 の発明によれば、前記第 1 の初期値と前記第 2 の初期値とを入力し、サイクル数が所定の数 k (k は、自然数) となった場合に第 1 のべき乗演算手段に $r = 2^{k-1}$ 、 $s = 2^r$ として s 乗を計算させる第 1 の制御信号と、第 2 のべき乗演算手段に $r = \{(m-1) \bmod (2^{k-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第 2 の制御信号とを入力し、前記乗算モジュールの選択手段には、 $(m-1)$ の 2 進表現でのビット $k-1$ が 1 の場合には前記第 2 のレジスタ手段の入力に前記第 2 の乗算手段の出力を入力し、 $(m-1)$ の 2 進表現でのビット $k-1$ が 1 でない場合には前記第 2 のレジスタ手段の入力に前記第 2 のレジスタ手段の出力を入力するための第 3 の制御信号を入力する、乗法逆元演算回路を含む装置が提供される。

【0052】本発明の請求項 22 の発明によれば、請求項 1 の乗算モジュール 2 個と、第 1 の初期値が設定できる第 1 のレジスタ手段と、第 2 の初期値が設定できる第 2 のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第 1 の出力を他の前記第 1 の入力部に接続し、前記乗算モジュールのそれぞれ第 2 の出力を他の前記第 2 の入力部に接続し、前記乗算モジュール群の結合によって得られた回路に対し、その第 1 の入力部に前記第 1 のレジスタ手段の出力が接続され、前記乗算モジュールの第 2 の入力部に前記第 2 のレジスタ手段の出力が接続され、前記乗算モジュールの第 1 の出力部に前記第 1 のレジスタ手段の入力が接続され、前記乗算モジュールの第 2 の出力部に前記第 2 のレジスタ手段の入力が接続された乗法逆元演算回路を含む、装置。

【0053】本発明の請求項 23 の発明によれば、3 個以上の請求項 1 の乗算モジュールと、第 1 の初期値が設定できる第 1 のレジスタ手段と、第 2 の初期値が設定で

20

きる第 2 のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第 1 の出力を他の前記第 1 の入力部に接続し、前記乗算モジュールのそれぞれ第 2 の出力を他の前記第 2 の入力部に接続し、前記乗算モジュール群の結合によって得られた回路に対し、その第 1 の入力部に前記第 1 のレジスタ手段の出力が接続され、前記乗算モジュールの第 2 の入力部に前記第 2 のレジスタ手段の出力が接続され、前記乗算モジュールの第 1 の出力部に前記第 1 のレジスタ手段の入力が接続され、前記乗算モジュールの第 2 の出力部に前記第 2 のレジスタ手段の入力が接続された乗法逆元演算回路を含む、装置が提供される。

【0054】本発明の請求項 24 の発明によれば、前記乗算モジュールの数 n (n は、自然数) は、 $[\log_2(m-1)+1]$ 以下とされる乗法逆元演算回路を含む装置が提供される。

【0055】本発明の請求項 25 の発明によれば、制御手段により、 i 段目 ($n \geq i \geq 1$) の乗算モジュールに対して、サイクル数が所定の数 q (q は自然数) となった場合に、 $p = \{n(q-1) + i\}$ として、第 1 のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第 1 の制御信号と、第 2 のべき乗演算手段に $r = \{(m-1) \bmod (2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算する第 2 の制御信号とを入力し、前記 i 番目の乗算モジュールの選択手段には、 $(m-1)$ の 2 進表現でのビット $p-1$ が 1 の場合には前記 i 番目の乗算モジュールの第 2 の出力に前記第 2 の乗算手段の出力を与え、 $(m-1)$ の 2 進表現でのビット $p-1$ が 1 でない場合には前記 i 番目の乗算モジュールの第 2 の出力を、前記 i 段目の乗算モジュールの第 2 の入力部からの m ビットデータとする第 3 の制御信号を入力する乗法逆元演算回路を含む、装置が提供される。

【0056】本発明の請求項 26 の発明によれば、 $[\log_2(m-1)+1]$ 個の請求項 1 の乗算モジュールと、それぞれの前記乗算モジュールを制御するための第 1 の制御信号群と、第 2 の制御信号群と、第 3 の制御信号群とを与える制御手段とを含み、前記乗算モジュールのそれぞれ第 1 の出力が他の前記乗算モジュールの第 1 の入力部に接続され、前記乗算モジュールのそれぞれ第 2 の出力が他の前記乗算モジュールの第 2 の入力部に接続されており、前記制御手段は、所定段目 k (k は、自然数) の乗算モジュールに対して、 $r = 2^{k-1}$ 、 $s = 2^r$ として s 乗を計算させる第 1 の制御信号を第 1 のべき乗演算手段に与え、 $r = \{(m-1) \bmod (2^{k-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第 2 の制御信号を第 2 のべき乗演算手段に与え、 $m-1$ の 2 進表現におけるビット $k-1$ が 1 の場合に選択手段の出力として第 2 の乗算手段の出力を与え、 $m-1$ の 2 進表現におけるビット $k-1$ が 1 でない場合には選択手段の出力として前記第 2 の入力部から入力される m ビットデータを与える乗法逆元演算回路を含む装置が提供される。

21.

【0057】本発明の請求項27の発明によれば、前記乗算モジュールに接続される対となったレジスタ手段を含む、乗法逆元演算回路が提供される。

【0058】本発明の請求項28の発明によれば、ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するため、第1の入力部から m ビットデータおよびべき乗演算手段からの出力を乗算手段に入力する段階と、第2の入力部からの m ビットデータおよび前記べき乗演算手段からの出力を乗算手段に入力する段階とを含む乗法逆元演算回路の制御方式であって、 $p = \{n(q-1) + i\}$ 10 として、第1のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第1の制御信号と、第2のべき乗演算手段に $r = \{(m-1) \bmod (2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算する第2の制御信号とを入力する段階と、 $m-1$ の2進表現におけるビット $k-1$ (k は、自然数)が1の場合に選択手段の出力として第2の乗算手段の出力を与え、 $m-1$ の2進表現におけるビット $k-1$ が1ではない場合には選択手段の出力として前記第2の入力部から入力される m ビットデータを与える段階とを含む、乗法逆元演算回路の制御方式が提供される。

【0059】本発明の請求項29の発明によれば、ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するため、第1の入力部から m ビットデータおよびべき乗演算手段からの出力を乗算手段に入力する段階と、第2の入力部からの m ビットデータおよび前記べき乗演算手段からの出力を乗算手段に入力する段階とを含む乗算方法を 30 実行させるためのソースコードが記録されたコンピュータ可読な記録媒体であって、該記録媒体は、 $p = \{n(q-1) + i\}$ として、第1のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第1の制御信号と、第2のべき乗演算手段に $r = \{(m-1) \bmod (2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算する第2の制御信号とを入力し、 $m-1$ の2進表現におけるビット $k-1$ (k は、自然数)が1の場合に選択手段の出力として第2の乗算手段の出力を与え、 $m-1$ の2進表現におけるビット $k-1$ が1ではない場合には選択手段の出力として前記第2の入力部から入力される m ビットデータを与える、記録媒体が提供される。

【0060】本発明の請求項30の発明によれば、ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するため、第1の入力部から m ビットデータおよびべき乗演算手段からの出力を乗算手段に入力する段階と、第2の入力部からの m ビットデータおよび前記べき乗演算手段からの出力を乗算手段に入力する段階とを含む乗算方法を 40 実行させるためのソースコードが記録されたコンピュータ可読な伝送媒体であって、該伝送媒体は、 $p = \{n(q-1) + i\}$ として、第1のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第1の制御信号と、第2のべき乗演算手段に $r = \{(m-1) \bmod$

22

$(2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算する第2の制御信号とを入力し、 $m-1$ の2進表現におけるビット $k-1$ (k は、自然数)が1の場合に選択手段の出力として第2の乗算手段の出力を与え、 $m-1$ の2進表現におけるビット $k-1$ が1ではない場合には選択手段の出力として前記第2の入力部から入力される m ビットデータを与える、伝送媒体が提供される。

【0061】本発明の請求項31の発明によれば、ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するため、第1の入力部からの m ビットデータおよびべき乗演算手段からの出力が 10 入力される乗算手段と、第2の入力部からの m ビットデータおよび前記べき乗演算手段からの出力が 20 入力される乗算手段とを含む暗号装置であって、 $p = \{n(q-1) + i\}$ として、第1のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第1の制御信号と、第2のべき乗演算手段に $r = \{(m-1) \bmod (2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算させる第2の制御信号とを入力するための手段と、 $m-1$ の2進表現におけるビット $k-1$ (k は、自然数)が1の場合に選択手段の出力として第2の乗算手段の出力を与え、 $m-1$ の2進表現におけるビット $k-1$ が1ではない場合には選択手段の出力として前記第2の入力部から入力される m ビットデータを与えるための手段と、を含む暗号装置が提供される。

【0062】本発明の請求項32の発明によれば、ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するため、第1の入力部からの m ビットデータおよびべき乗演算手段からの出力が 30 入力される乗算手段と、第2の入力部からの m ビットデータおよび前記べき乗演算手段からの出力が 40 入力される乗算手段とを含む誤り訂正復号器であって、 $p = \{n(q-1) + i\}$ として、第1のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第1の制御信号と、第2のべき乗演算手段に $r = \{(m-1) \bmod (2^{p-1})\} + 1$ 、 $s = 2^r$ として s 乗を計算する第2の制御信号とを入力するための手段と、 $m-1$ の2進表現におけるビット $k-1$ (k は、自然数)が1の場合に選択手段の出力として第2の乗算手段の出力を与え、 $m-1$ の2進表現におけるビット $k-1$ が1ではない場合には選択手段の出力として前記第2の入力部から入力される m ビットデータを与えるための手段と、を含む誤り訂正復号器が提供される。

【0063】本発明の請求項33の発明によれば、ガロア体 $GF(2^m)$ ($m \geq 1$) 上の m ビットデータを乗算するため、第1の入力部からの m ビットデータおよびべき乗演算手段からの出力が 50 入力される乗算手段と、第2の入力部からの m ビットデータおよび前記べき乗演算手段からの出力が 60 入力される乗算手段とを含む装置であって、 $p = \{n(q-1) + i\}$ として、第1のべき乗演算手段に $r = 2^{p-1}$ 、 $s = 2^r$ として s 乗を計算させる第1の制御信号と、第2のべき乗演算手段に $r = \{(m-1)$

$\text{mod}(2^{p-1}) + 1$ 、 $s = 2^r$ として s 乗を計算する第2の制御信号とを入力するための手段と、 $m-1$ の2進表現におけるビット $k-1$ (k は、自然数)が1の場合に選択手段の出力として第2の乗算手段の出力を与え、 $m-1$ の2進表現におけるビット $k-1$ が1ではない場合には選択手段の出力として前記第2の入力部から入力される m ビットデータを与えるための手段と、を含む装置が提供される。

【0064】

【発明の実施の形態】以下、本発明の図面に示した実施例をもって説明する。本発明においては、 $Hw(x)$ は x の2進表現におけるハミング重み、 $[x]$ は x の整数部(小数部を切り捨てた数)、 a は、 $GF(2^m)$ の原始多項式の根、 a^0 は、 $GF(2^m)$ における1、 M は乗算回路のレイテンシを表わすものとする。また、レジスタ $R1$ および $R2$ (これらについては後述)へ値を設定してから、次に値を設定するまでの期間を、1サイクルとする。

【0065】図4の乗算モジュール(基本演算モジュール)を用い、順序回路として乗法逆元演算回路を構成する場合は図5または図6のように、組み合わせ回路として実現する場合は図7のように回路を構成する。図5ないし図7における基本モジュール等の制御信号は、図8のように与える。図6における制御信号については後述する。また、後述する図12のようにパイプライン化することもできる。

【0066】ここで、基本的な乗算モジュールは、2個の乗算回路と2個の2のべき乗演算回路(2^k乗演算を行う)、および出力 B のセレクトで構成される。各べき乗演算回路において k をいくつにとるかは、モジュールの制御信号として外部より与えられる(図4)。順序回路として実現する場合(図5、図6)、図4の乗算モジュールを1個以上用い、その出力をレジスタに接続する。レジスタは初期値が設定できるものを用い、その初期値は外部より与えられる。レジスタ出力は乗算モジュール群の入力へフィードバックされる。乗算モジュールやセレクトの制御は、専用の制御手段、例えばコントロール回路によって行う。そのコントロール回路は、図8の手順に従って各制御信号を生成する。

【0067】図8のアルゴリズムを回路として実装する実施例について説明する。このアルゴリズムから得られるデータフローグラフを、回路実装に用いる。各部品を組み合わせ回路で構成したうえでデータフローグラフ全体を静的に回路展開すれば組み合わせ回路が得られるし、リソースアロケーションとスケジューリングを行って順序回路とすることもできる。順序回路とする場合、乗算やべき乗演算などは必ずしもパラレル入出力である必要はない。

【0068】なお、上記アルゴリズムでは

【0069】

【数10】

$$(m-1) \bmod (2^{k-1})$$

などと剰余演算を行っているように見える個所があるが、これは実際には「 $m-1$ の2進表現のうち下位 $k-1$ ビットを抽出する」操作で、きわめて軽いハードで実現できる(組み合わせ回路にする場合は、これらは定数値となるので、事前計算による回路簡単化が可能)。また、2のべき乗演算も簡単な回路で作れるので基本的に乗算とレジスタだけのコストと考えてよい。

10 【0070】さて、このアルゴリズムを順序回路化したとき、 m が動的に変化できるようにするのは簡単である。レジスタは m によらず $R1$ と $R2$ の2つであり、それらの役割が m によって変わることはない。 m に依存して変化するのは、ループの回数と、べき乗演算のべき数だけであり、データパスの構造は m にほとんど依存しない。データパスをコントロールするために、 m からべき数

【0071】

【数11】

$$20 \quad \{(m-1) \bmod (2^{k-1}) + 1\}$$

の動的導出をしなければならないが、それはきわめて容易で、上記のとおり $m-1$ の2進表現からビットを切り出すだけで行える。

【0072】組み合わせ回路として実現する場合(図7)、図4の基本構成モジュールを直列に、

【0073】

【数12】

$$[\log_2(m-1)] + 1$$

30

個接続する。各モジュールの制御信号は、図8の手順に従って与えられる。その制御信号は m を固定すれば固定値となるので、それにより論理を簡単化できる。なお、 m を別のレジスタで持っておき、そこから制御信号をデコードすることにより、任意の m に対処できるような回路を構成してもよい。

【0074】図5の変形として、乗算モジュールを下記式

【0075】

40 【数13】

$$[\log_2(m-1)+1] \geq n \geq 1$$

の範囲内の n 個を直列に接続して得られる回路に、図5と同様にレジスタと各モジュールの制御回路を付加して回路を構成することもできる(図6)。その q (q は、自然数)サイクル目において、 i 段目($n \geq i \geq 1$)のモジュールの制御入力には、図8の $n(q-1) + i$ サイクル目の制御信号を与える。たとえば、3段直列に接続した場合、1段目のモジュールには図8の1, 4, 7, ...サイクル目の制御信号、2段目のモジュールには2,

50

5, 8, ... サイクル目の制御信号、3 段目のモジュールには 3, 6, 9, ... サイクル目の制御信号を、サイクルごとに与える。

【0076】なお、本発明は、図 4、図 5、図 6、図 7、図 12 から冗長論理を削除して得られる回路をすべて含む。とくに、一方の入力に常に定数 a^0 が与えられる乗算回路は削除し、他方の入力をその出力と直結する。また、出力が使われないべき乗演算回路や、出力が固定の選択回路も削除する。さらに、図 4 において、乗算回路やべき乗演算回路などは必ずしも組み合わせ回路

である必要はない。

【0077】 $m=15$ の組み合わせ回路を例に、実際にどのような制御信号をモジュールに与えるかを図 9 に示す。

【0078】 $m=15$ の場合、基本モジュールを 4 つ直列につなげた構造となる。モジュール番号を、入力側から 1, 2, 3, 4 とする。このとき、図 9 に示すようにたとえばモジュール 2 には次のような制御信号を与える。

○べき乗演算回路 1 は、4 乗演算を行う。

○べき乗演算回路 2 は、2 乗演算を行う。

○選択回路は、出力 B に入力 B の値を出す。

他のモジュールについても同様である。ここで、モジュール 1, 2 の乗算回路 2、モジュール 4 の乗算回路 1、モジュール 1 のべき乗演算回路 2、モジュール 4 のべき乗演算回路 1 は、いずれも不要となるので削除し、それによって得られた回路を用いる。

【0079】 $m=15$ で、図 5 のような順序回路として実現する場合、レジスタを初期化した後、4 サイクルかけて処理を行う。基本回路モジュールへの制御信号は、

$Fermat : \{[\log_2(m-2)]+1\} \times \text{乗算器のレイテンシ}$

伊東 $: \{[\log_2(m-1)]+Hw(m-1)-1\} \times \text{乗算器のレイテンシ}$

本手法 $: [\log_2(m-2)]+1 \times \text{乗算器のレイテンシ}$

で、 $Fermat$ と本手法がもっとも良い。伊東のアルゴリズムと本手法のレイテンシの違いを、図 10 のグラフに示す。

【0083】以上をまとめると、本手法は、回路サイズを伊東と同じで $Fermat$ よりはるかに少なく保ったまま、伊東の約半分の ($=Fermat$ と同じ) レイテンシに改善できる。また、図 6 下段のとおり、実際に汎用論理合成ツールで実回路を作成した場合にも、上記アルゴリズムの差がそのままゲート数や速度に現れる。図 11 には、本発明において、 $m=14, 15, 16$ とした場合のデータフロウグラフを示す。

【0084】図 12 には、本発明の乗法逆元演算回路のさらに別の実施例を示す。図 12 の乗法逆元演算回路は、図 7 に示した実施例の構成に加えて、レジスタ $R1, R2$ が追加されている。これらの対となったレジスタ $R1, R2$ は、図 12 に示した乗法逆元演算回路を構成する乗算モジュールのいかなる位置においても、また

図 9 におけるモジュール 1, 2, 3, 4 と同じものをこの順に与える。制御信号の生成は、図 5 におけるべき乗レジスタ入力制御信号生成回路で行う。

【0080】他の m についても、同様に基本モジュールの接続と制御を行う。

(1) 図 5 のように順序回路として実装した場合：計算にかかるサイクル数は、任意の m に対し、

$Fermat : m-2$

伊東 $: [\log_2(m-1)]+Hw(m-1)-1$

本発明 $: [\log_2(m-1)]+1$

で、本発明がもっとも良く、最大で伊東の約半分で計算できる。

たとえば $m=192$ の場合

$Fermat : 190$

伊東 $: 13$

本発明 $: 8$

また、 $m=511$ の場合、

$Fermat : 509$

伊東 $: 15$

20 本手法 $: 9$

となり、大きくレイテンシが改善される。

【0081】(2) 図 7 のように組み合わせ回路として実装した場合：乗算回路の個数 (回路サイズ) は、任意の m に対し、

$Fermat : m-2$

伊東 $: [\log_2(m-1)]+Hw(m-1)-1$

本発明 $: [\log_2(m-1)]+Hw(m-1)-1$

で、伊東と本手法がもっとも良い。

【0082】また、レイテンシ (スピード) は、

いかなる個数でも配置することができる。

【0085】

【発明の効果】上述したように、本発明によれば、基本モジュールを組み合わせた形で、低いレイテンシ (順序回路の場合は少ない処理クロック数、組み合わせ回路の場合は少ディレイ) を乗算回数を増やすことなく達成することができる。

【0086】本手法では、動的に m を変えるのが、 $Fermat$ と同程度に容易である (順序回路として実装した場合)。レジスタの個数が 2 個と静的に決まっているので、任意の m でほぼ同じデータパスが使える、ループ回数などのコントロールを変更するだけで m を変更できる。コントロールを動的に変更するのも先述のとおり簡単な回路でできる。本手法は、逆元演算のみならず、べき乗演算の高速化に応用できる。

【0087】本手法は、文献 [4] 等にある Composite Field ベースの高速化手法と組み合わせることで、より一層

の回路規模縮小／レイテンシ短縮を実現できる。これまで本発明の図面に示した実施例をもって説明してきたが、本発明は図面に示した実施例に限定されるものではなく、種々の変更、除外、別の態様が可能である。また、本発明を適用することができる装置は、暗号装置、誤り復号装置ばかりではなく、ガロワ拡大体を用いるいかなる装置に対しても適用できることは言うまでもないことである。

【図面の簡単な説明】

【図 1】 Fermat の定理を用いた従来の乗法逆元演算のアルゴリズムを示した図。

【図 2】 従来の乗法逆元演算のアルゴリズムを木構造を用いて示した図。

【図 3】 従来の乗法逆元演算のアルゴリズムを示した図。

【図 4】 本発明の乗法モジュールを示した図。

【図 5】 本発明の乗法逆元演算回路を示した図。

【図 6】 本発明の乗法逆元演算回路の別の実施例を示した図。

【図 7】 本発明の乗法逆元演算回路のさらに別の実施例を示した図。

【符号の説明】

- u 1 … 第 1 のべき乗演算手段
- u 2 … 第 2 のべき乗演算手段
- u 3 … 第 1 の乗算手段
- u 4 … 第 2 の乗算手段
- u 5 … 選択手段
- S 0 … 第 3 の制御信号
- S 1 … 第 1 の制御信号
- S 2 … 第 2 の制御信号
- R 1 … 第 1 のレジスタ手段
- R 2 … 第 2 のレジスタ手段

【図 1】

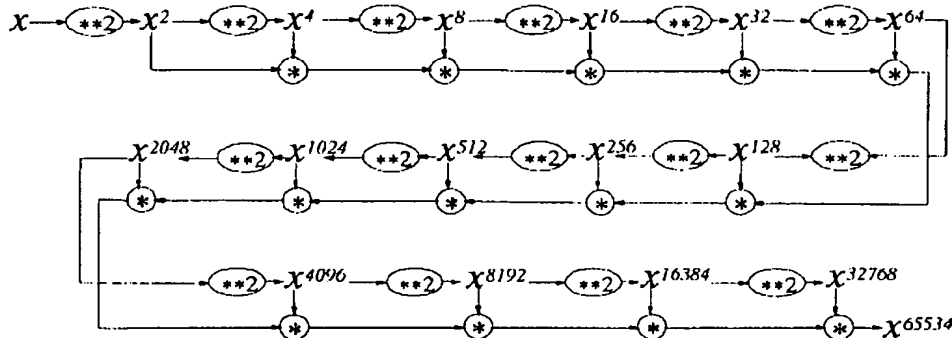


図1 Fermatの定理による計算過程の例(m=16)

【図 4】

基本演算モジュール

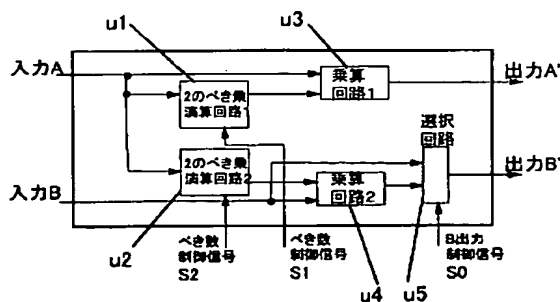
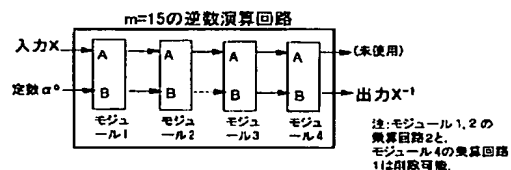


図4 回路の構成に用いる乗算デバイス

【図 9】



	べき数制御S1	べき数制御S2	出力B制御S0
モジュール 1	2 ¹ 乗	(べき数不要)	入力B
モジュール 2	2 ² 乗	2 ¹ 乗	入力B
モジュール 3	2 ⁴ 乗	2 ³ 乗	乗算回路2出力
モジュール 4	(べき数不要)	2 ⁷ 乗	乗算回路2出力

図9 各モジュールへ与える制御信号の具体例(m=15)

【図 2】

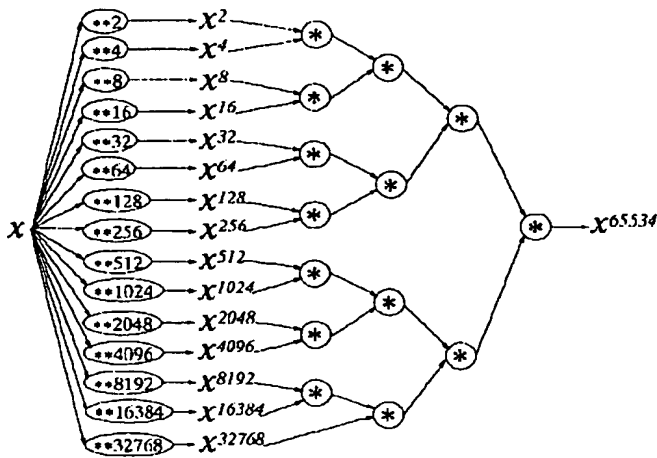


図2 Fermatの定理による計算過程の例(m=16)

【図 3】

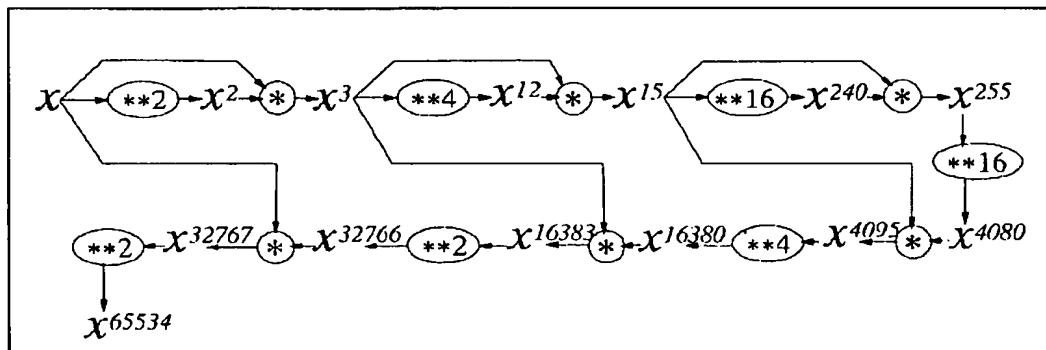


図3 伊東・辻井のアルゴリズムによる計算過程の例(m=16)

【図 8】

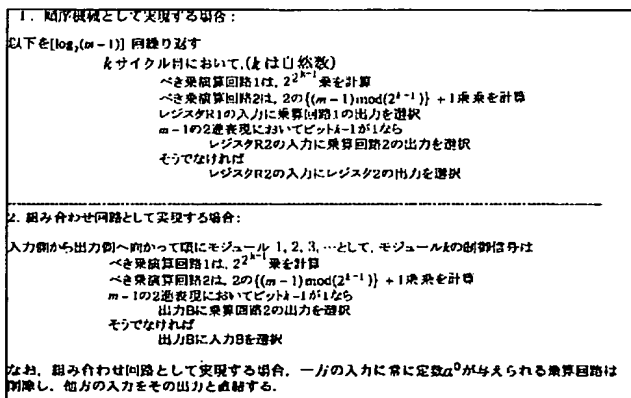
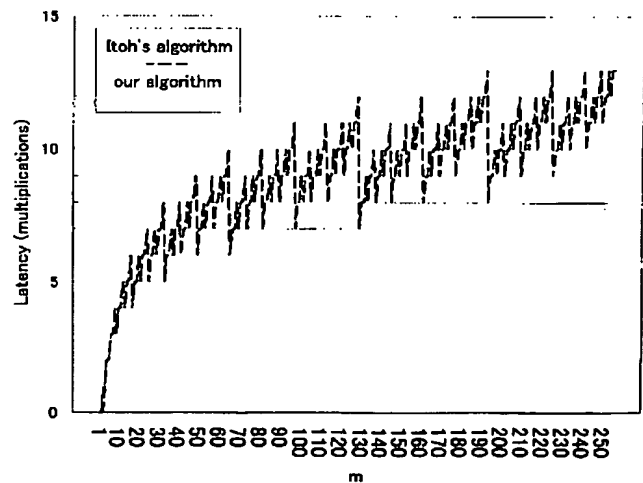


図8 各モジュールの制御信号の具体的な生成法

【図 10】



【図 5】

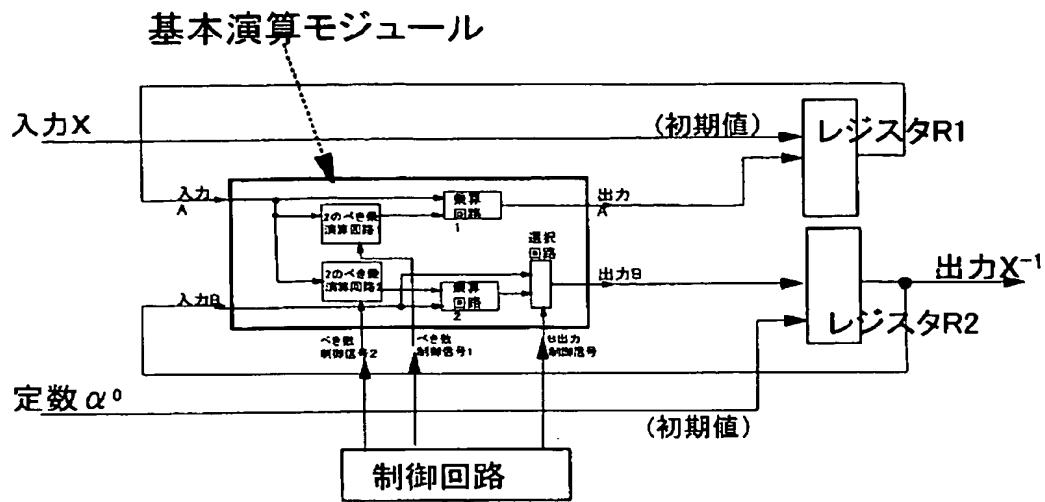


図5 順序機械として実現する場合の全体構成法1

【図 6】

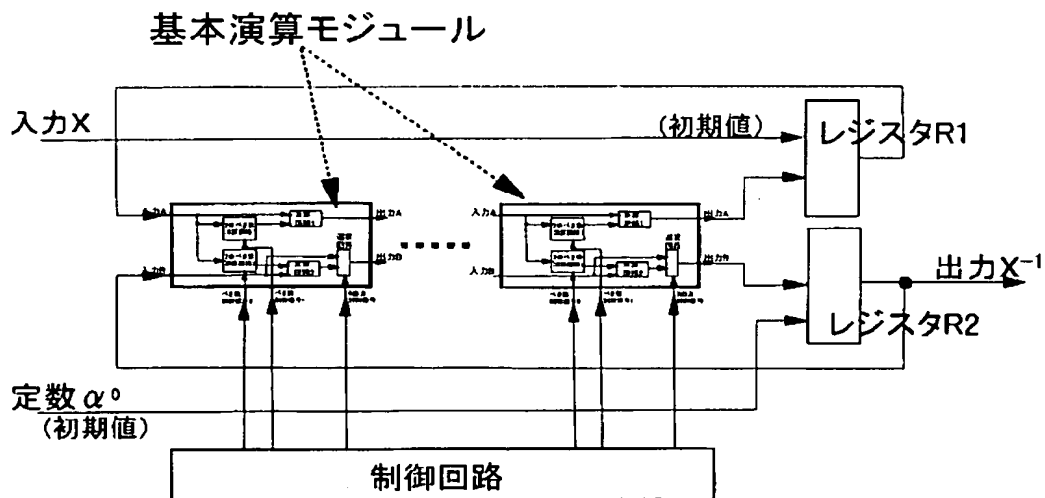


図6 順序回路として実現する場合の全体構成法2

【図 7】

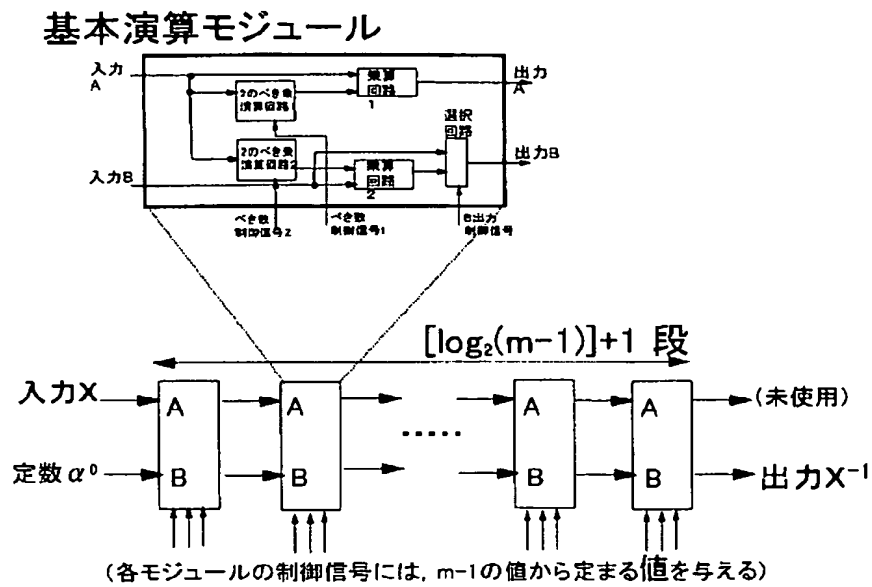
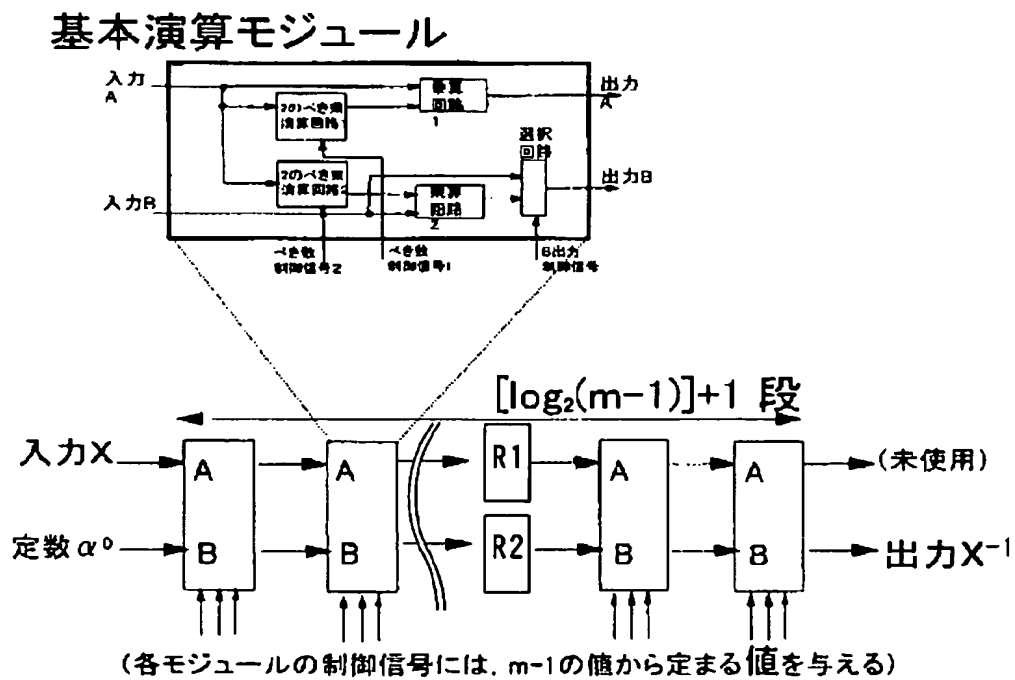
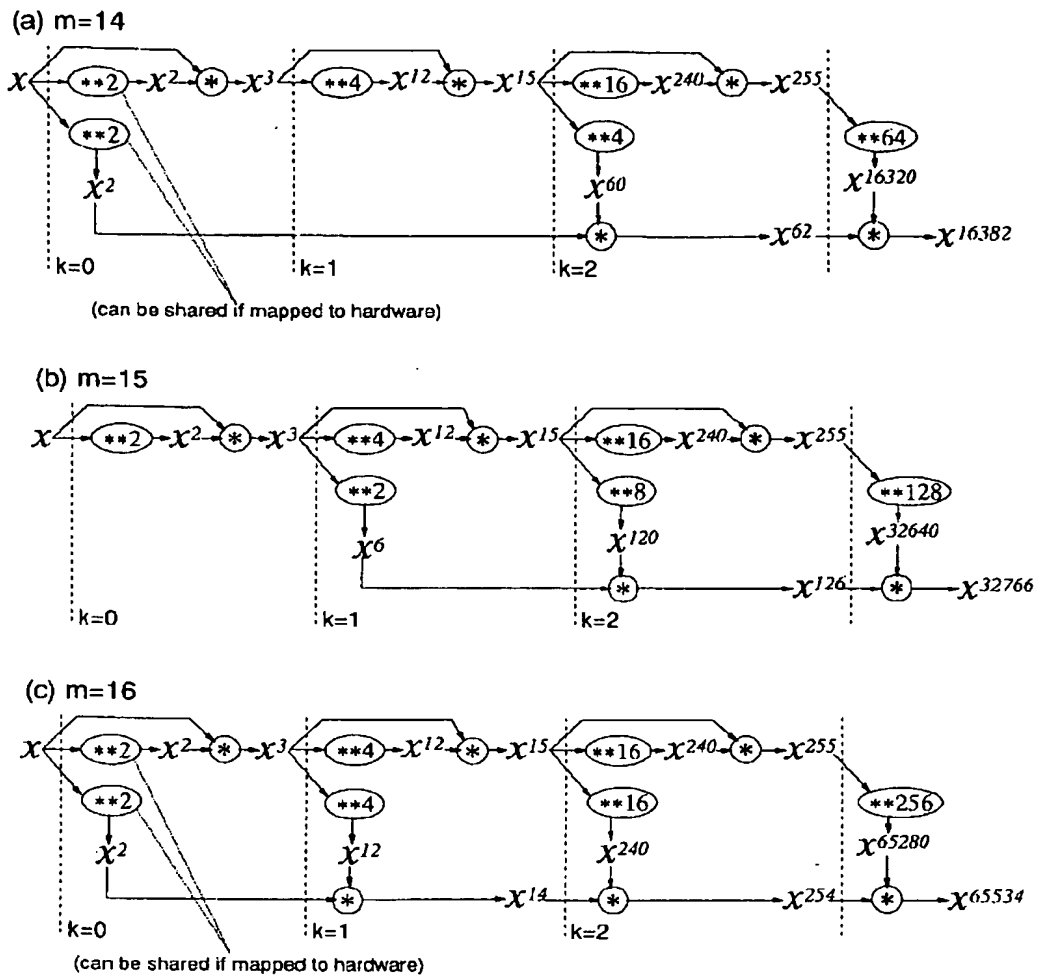


図7 組み合わせ回路として実現する場合の全体構成法

【図 12】



【図 11】



【手続補正書】

【提出日】平成13年5月1日(2001.5.1)

【手続補正1】

【補正対象書類名】図面

【補正対象項目名】図5

【補正方法】変更

【補正内容】

【図5】

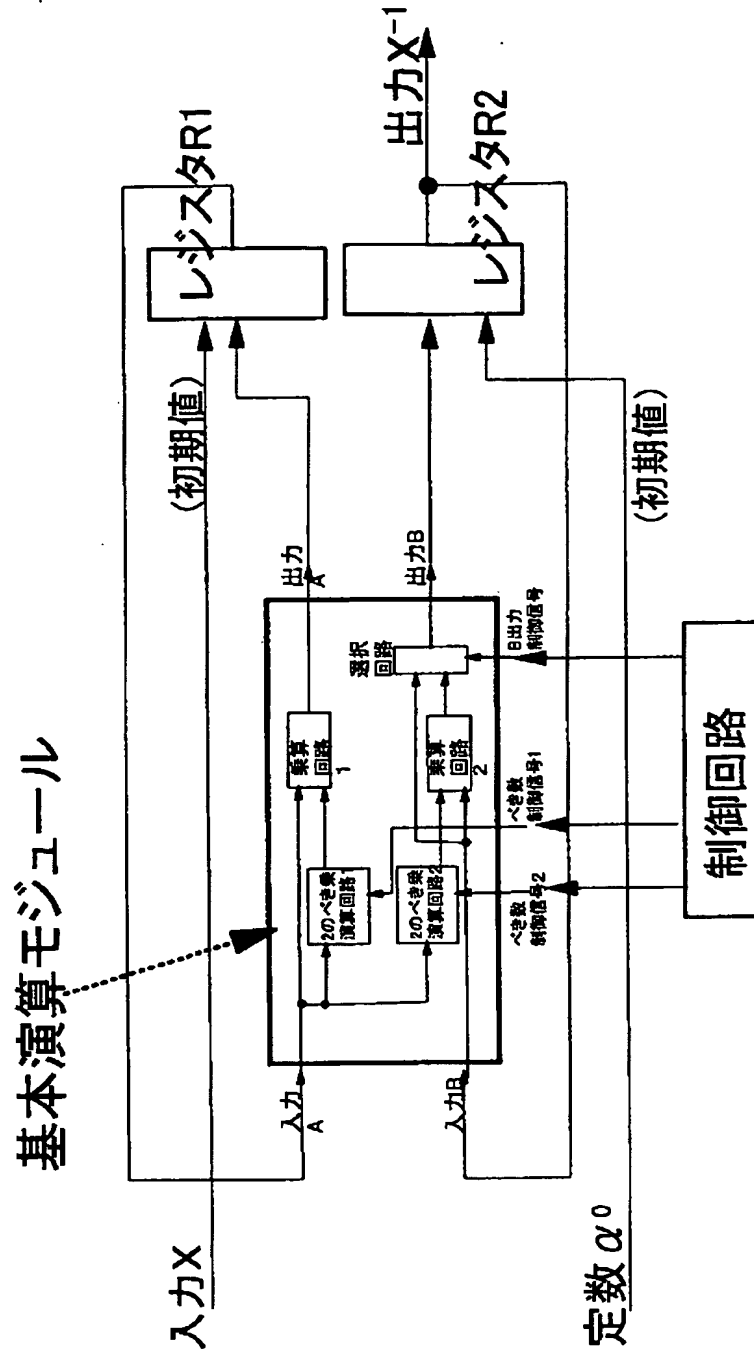


図5 順序機械として実現する場合の全体構成法1

【手続補正2】

【補正対象書類名】図面

【補正対象項目名】図6

【補正方法】変更

【補正内容】

【図6】

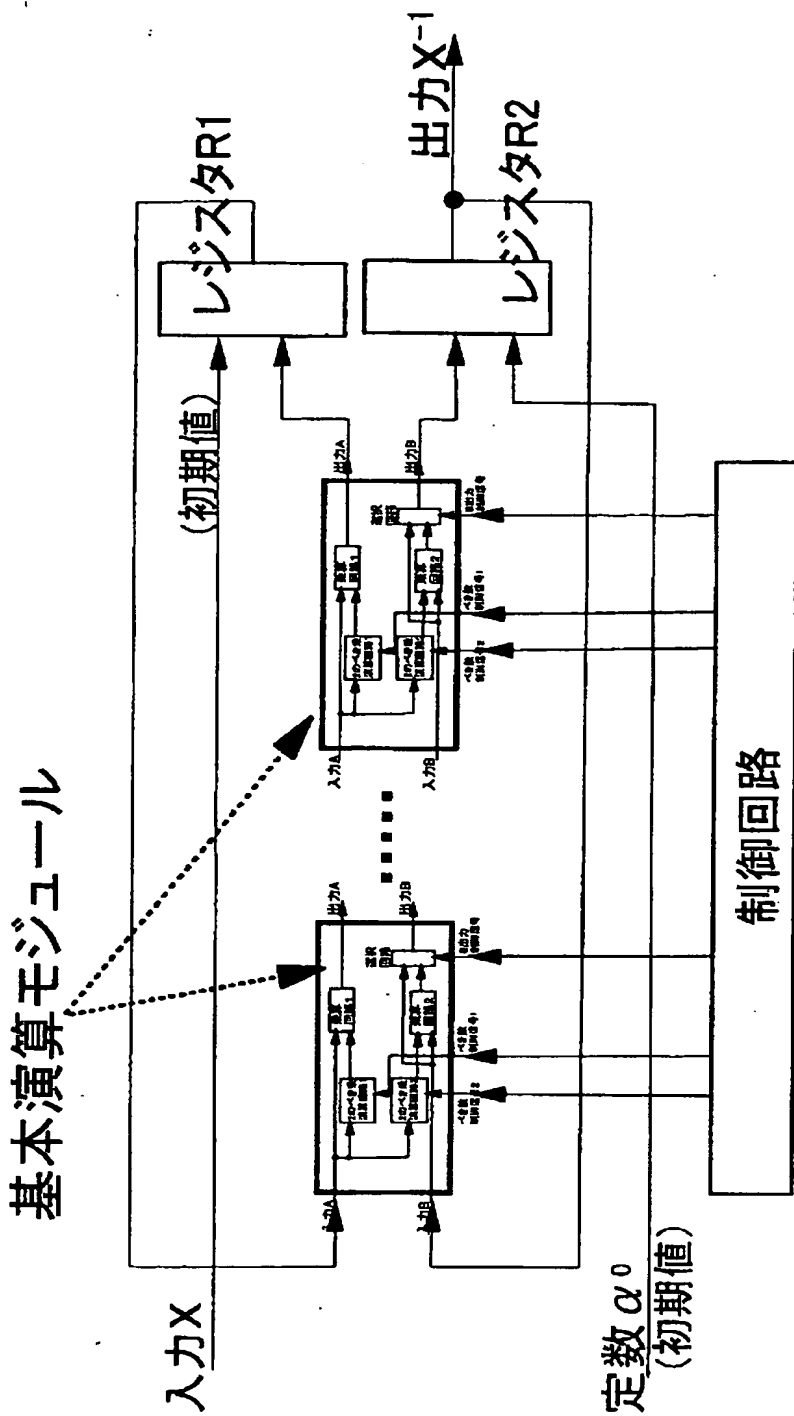


図6 順序回路として実現する場合の全体構成法2

【手続補正3】
 【補正対象書類名】図面
 【補正対象項目名】図7

【補正方法】変更
 【補正内容】
 【図7】

基本演算モジュール

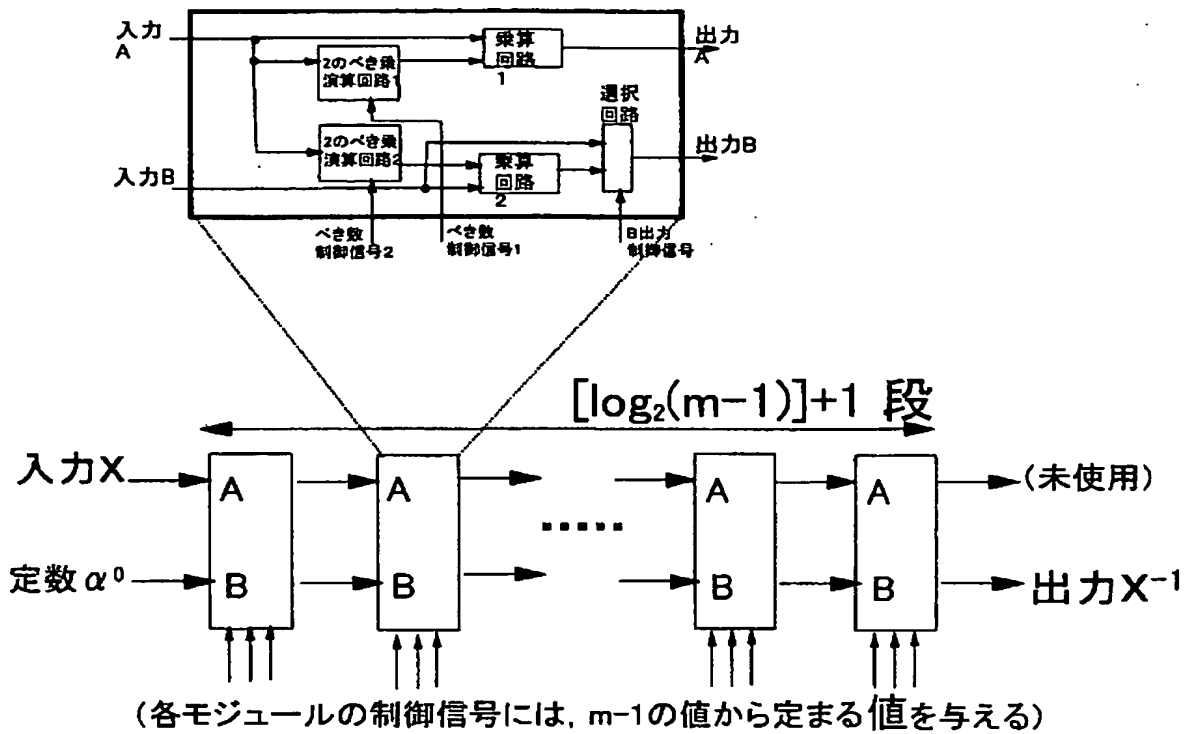


図7 組み合わせ回路として実現する場合の全体構成法

フロントページの続き

(72)発明者 森岡 澄夫
神奈川県大和市下鶴間1623番地14 日本ア
イ・ビー・エム株式会社 東京基礎研究所
内

(72)発明者 片山 泰尚
神奈川県大和市下鶴間1623番地14 日本ア
イ・ビー・エム株式会社 東京基礎研究所
内

Fターム(参考) 5J104 AA22 NA18